公開資料

企画調査終了報告書

研究開発プログラム「犯罪からの子どもの安全」

プロジェクト企画調査名
「ITを用いた子どもの安全確保の研究開発」

調査期間　平成１９年１０月～平成２０年３月

研究代表者　　松本　勉

所属、役職　　国立大学法人横浜国立大学大学院環境情報研究院　教授

１．企画調査課題

(1)研究代表者　　：　松本　勉

(2)企画調査課題名　：　ITを用いた子どもの安全確保の研究開発

(3)企画調査期間　　：　平成１９年１０月～平成２０年３月

２．企画調査構想

(1)　背景

近年、携帯電話の出会い系サイトやインターネットの掲示板を介して子どもが犯罪に巻き込まれる事件が多発している。警察庁によると、「出会い系サイト」を利用した犯罪の被害にあった18歳未満の被害児童は、平成18年度には1,153人に上り、その内、携帯電話を使用した被害児童は1,114人で96.6%を占めている。NTTドコモモバイル社会研究所の調査によると、子どもの携帯電話保有率は、小学生は24.1%、中学生は66.7%、高校生は96.0%にも上る。「持っていないが、欲しい」を加えると、小学生は77.7%、中学生も95.2%となり、子どもの携帯電話の保有数は今後も増大すると予想される。また、今後、日記／ブログ、SNSが普及すると、携帯電話を利用してインターネットにアクセスする子どもが犯罪に巻き込まれる確率はより高くなると考えられる。

そこで、われわれは、主に携帯電話によって構成されるサイバー空間とリアル空間の両面から子どもが犯罪やトラブルに巻き込まれる予兆を検出し、子どもの安全を確保するためのシステムを開発する「ITを用いた子どもの安全確保」のためのシステムを開発することを検討している。本システムでは、サイバー空間における子どものコミュニケーション行動をモニタリングして子どもが犯罪やトラブルに巻き込まれる予兆データを察知し、リアル空間における危険情報や子どもの行動情報をモニタリングすることにより、子どもが犯罪やトラブルに巻き込まれないように子ども本人や関係者に対して対応策を提供するものである。

URLフィルタリング等のペアレンタルコントロール（Parental Control）がサイバー空間への入り口の対策技術であるのに対して、提案システムは実際に危険が子どもに及ぶ間際でアラートを発する技術である。また、頻繁にURLが変わる危険サイトへの対応やSNS等の必ずしも危険サイトとは言い切れない場合への対応も柔軟にできるといった、フィルタリング技術にはない特長を有する。本システムの開発の目標は、犯罪やトラブルに発展しそうな前兆を高い割合で予測することであり、ITにおける対応策が子ども本人や親にとっての子どもに対する犯罪不安度を大幅に軽減する仕組みを提供することである。

(2)　企画調査の目的

企画調査においては、提案するシステムの実現可能性を明確にすることを目的として、以下の事項につき検討することとした。

・ 携帯電話を含む子どものインターネット利用状況と危険事例

子どもが犯罪に巻き込まれる予兆を検知するための基礎データ収集として、子どものインターネット・携帯電話利用状況ならびに犯罪に巻き込まれた事例やヒヤリハット事例の調査を行う。調査手法としては小中高校生、父兄へのアンケート及び養護教員を中心とするヒアリング調査を実施する。

・ サイバー／リアル空間モニタリング情報分析手法

提案するシステムの具体化を行うために、PCおよび携帯電話を用いて、インターネット上のサービス（SNS、出会い系等）を利用し、サイバー空間でやり取りされる情報を捕捉すると共に、携帯電話の位置検索サービスから取得できる位置情報を利用し、具体的な危険パターンの導出を行う。また、導出された危険パターンを自動的に検出するためのアルゴリズムの検討を、データマイニング、推論等のアルゴリズムの調査を行った上で検討する。

・ 実証実験の体制

システムの有効性を検証する実証実験の実現性を明確にするために、実証実験フィールドの選定、インターネットサービス事業者および通信事業者の選定、実証実験実施にあたっての課題抽出と解決法の検討について検討を行う。

(3) 企画調査実施スケジュール

企画調査の実施スケジュールを以下に示す。

実施項目	平成１９年度 （６ヶ月） H19.10～H20.3					
	10	11	12	1	2	3
携帯電話を含む子どものインターネット利用状況と危険事例調査	←―――	―――	―――	―――	―――	―――
サイバー／リアル空間モニタリング情報分析手法調査	←―――	―――	―――	―――	―――	―――
実証実験の体制検討		←―――	―――	―――	―――	
まとめ・プロジェクト提案書作成						←―――

(4) 企画調査実施状況

企画調査の実施状況を下表に示す。

実施項目	実施状況
携帯電話を含む子どものインターネット利用状況と危険事例調査	現場職員、大学2年生、中学生へのヒアリングを実施した。 また、神奈川県下の中学校2校、高校1校に対してアンケート調査を実施し、中学生のアンケートについて集計し、分析を行った。 （高校生へのアンケートについては集計中である。）
サイバー／リアル空間モニタリング情報分析手法調査	サイバー空間モニタリング手法、ならびにリアル空間モニタリング手法について詳細化を実施した。 特にサイバー空間モニタリング手法については、システム構成図（案）を示した。
実証実験の体制検討	実証実験フィールドとして、アンケート実施校を候補とすることとした。また、通信事業者との連携として、情報通信研究機構（NICT）が某通信事業者とパートナー契約を結んでおり、システム開発の面で問題ないとの結論に達した。 提案システムの法的課題については、弁護士からの、「携帯電話に関する契約が、親と携帯電話事業者の間で行われれば、子供の通信内容を収集することに関する契約上の問題はないが、子供は未成熟であっても個人であるため、基本的には告知を行ったほうがよい」との見解をいただいた。

(5)　外部発表等

①招待、口頭講演　（国内　2件、海外　0件）

- 松本 勉（横浜国立大学）、富井尚志（横浜国立大学）、物部博文（横浜国立大学）、中川裕志（東京大学）、滝沢修（情報通信研究機構）、井上大介（情報通信研究機構）、赤井健一郎（三菱総合研究所）、佐藤明男（三菱総合研究所）、村瀬一郎（三菱総合研究所）、“ITを用いた子どもの安全確保の構想”、2008年暗号と情報セキュリティシンポジウム、4E1-3、フェニックス・シーガイア・リゾート　ワールドコンベンションセンターサミット、2008年1月22日～25日。

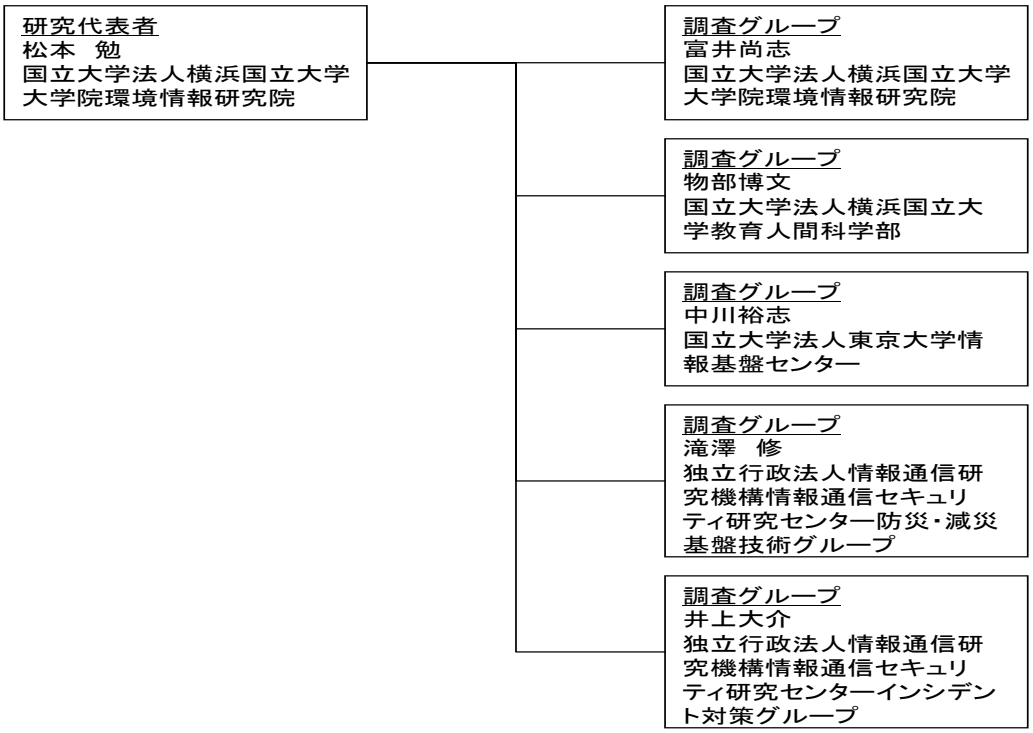
- 松本 勉、“サイバー空間で子供を守るために”、NICT情報通信セキュリティシンポジウム「ネットワーク時代のプライバシとセキュリティ」、SYDホール、2008年2月28日。

②ポスター発表　　（国内　1件、海外　0件）

- パネル展示「ITを用いた子どもの安全確保の研究開発」、2007年度日本大学文理学部特別展　「安全を科学する－最新の防犯技術と科学捜査－」2007年12月08日～24日。

３．企画調査実施体制

(1)　体制



(2)　メンバー表

①調査グループ（全体が１グループである）

氏　名	所　属	役　職	研究項目	参加時期
松本　勉	国立大学法人横浜国立大学 大学院環境情報研究院	教授	全般	平成19年10月～ 平成20年3月
富井尚志	国立大学法人横浜国立大学 大学院環境情報研究院	准教授	全般	平成19年10月～ 平成20年3月
物部博文	国立大学法人横浜国立大学 教育人間科学部	准教授	全般	平成19年10月～ 平成20年3月
中川裕志	国立大学法人東京大学 情報基盤センター	教授	全般	平成19年10月～ 平成20年3月
滝澤　修	独立行政法人情報通信研究機構情報通信セキュリティ研究センター防災・減災基盤技術グループ	グループリーダー	全般	平成19年10月～ 平成20年3月
井上大介	独立行政法人情報通信研究機構情報通信セキュリティ研究センターインシデント対策グループ	研究員	全般	平成19年10月～ 平成20年3月

４．実施内容及び成果

(1) 携帯電話を含む子どものインターネット利用状況と危険事例調査

企画調査計画書における記載

子どもが犯罪に巻き込まれる予兆を検知するための基礎データ収集として、子どものインターネット・携帯電話利用状況ならびに犯罪に巻き込まれた事例やヒヤリハット事例の調査を行う。調査手法としては小中高校生、父兄へのアンケート及び養護教員を中心とするヒアリングを行う。本調査については、専門の調査会社に調査を依頼し、調査グループの指導のもと作業を進めることとする。

【子どもへのアンケート】
対象：横浜市内の小・中・高校　各3校の児童・生徒合計計100名以上
設問内容：
インターネット利用状況
- 利用頻度
- 使用しているサービス（メール、SNS、ブログ、出会い系等）
- ネットを通じての出会い（友人、恋人等）
- ネットを通じての嫌な体験・トラブル

・ 携帯電話利用状況
- 利用の有無
- 使用しているサービス（メール、SNS、ブログ、出会い系等）
- ネットを通じての出会い（友人、恋人等）
- ネットを通じての嫌な体験・トラブル

・ 犯罪に巻き込まれた事例およびヒヤリハット事例
- 知らない人に声をかけられた事例および場所
- 誘拐
- いじめ
- 痴漢
- 等

・ 子どもの社会的・心理的状態
- 自尊感情
- 学校不適応
- 学校満足度
- 社会的スキル
- 親に対する満足度など

【保護者へのアンケート】
対象：横浜市内の小中高校生を持つ保護者　50人程度
＊上記「子どもへのアンケート」での回答者の保護者を想定する。
設問内容：
・ 子どもに対して不安に思うこと
- インターネット
- 携帯電話
- 登下校
- 学校（いじめ等）

・ 子どもが遭ったヒヤリハット事例
- 知らない人に声をかけられた事例および場所
- 誘拐

- いじめ
- 痴漢
- 等

【養護教員を中心とする教員へのヒアリング】
対象：横浜市内の小中高校　教員　10名以上
質問内容：
- ご自身の所属する学校での児童または生徒のPC・携帯電話所有状況
- インターネットを介してのトラブル事例（いじめ、誹謗中傷、出会い系等）
- インターネットを介さないトラブル事例（恐喝、誘拐、強姦等）

子どもへのアンケートおよびヒアリング、保護者へのアンケート、現場教員へのヒアリングを通して、子どものインターネット利用状況、携帯電話利用状況、危険・ヒヤリハット事例、教員や親の想い等を調査したため、その成果を述べる。

なお、実施計画書には、本調査において、子どもへのアンケート、保護者へのアンケート、養護教員を中心とする教員へのヒアリングを挙げたが、このうち、保護者へのアンケートは未実施である。これは以下の理由による。

- 学校を通して要請したが、学校側の調整が進まなかった
- そのため、保護者へのアンケートに代えて子どもへのヒアリングを実施することにより有益な情報が得られた

1)　現場教員へのヒアリング

＜背景と目的＞

現場教員のヒアリングに先立ち，神奈川県教育委員会の生徒指導担当部署へ「IT に関連した児童生徒の危険行動」についての聞き取り調査を実施した。その結果，①個人情報保護の観点から事例等の情報公開が難しいこと，②教育委員会で把握している事例は，警察等を通して表明化した事例が主体であり，実際には学校から報告されていない案件が相当数予測されること、③教育委員会、神奈川県警、研究者の３者の連携により対策を実施していること、等が確認された。

そこで，小中高等学校を対象とした調査や実証実験の実施に際して、協力を得なければならない教員にヒアリングを実施し，本プロジェクト研究における課題を明らかにしようと試みた。すなわち，神奈川県下，横浜市，川崎市の小中学校現職教員を対象に①児童生徒の IT の利用状況、②IT に関連した児童生徒の危険行動の実態や具体的な事例，③犯罪に巻き込まれるような児童生徒の特性、④実証実験の可能性と児童生徒および保護者への指導方法等について、ヒアリングを行い、実態把握および実証実験の進行にかかわる問題点の洗出しをすることを、本ヒアリングの目的とした。

＜ヒアリングの内容＞

実施日	2007年11月21日（水）
実施場所	横浜国立大学　物部研究室
対象者	神奈川県公立　小、中学校に在籍する教員4名
インタビュア	横浜国立大学　物部 三菱総研　　村瀬、佐藤、赤井

調査内容	結果
携帯電話、インターネットの利用状況	・携帯電話、インターネットを通して危険にさらされる児童・生徒は増加傾向である。 ・男子児童・生徒は、自殺サイトなどのマニアックなものに走る傾向がある。 ・女子児童・生徒は、出会い系サイトを利用する傾向がある。 ・女子中学生では、ブログ・プロフはかなり利用されている。 ・SNSは女子児童・生徒がはまりやすい。 ・中学3年生くらいで、メールを頻繁にやり取りする、ネット依存的な傾向がある子が多い。
子どもの危険行動パターン	・小学校高学年の女子児童が、出会い系で実際に呼び出しをして遠くから見ていた事例がある。 ・依存傾向の強い（女子）児童が優しい言葉にだまされる事例がある。
犯罪に巻き込まれる子どもの特性	・精神的に問題がある子どもよりも、あっけらかんとしている子どものほうがネットを利用し、軽い考えで犯罪に巻き込まれていく傾向がある。
犯罪に巻き込まれたケース、ヒヤリハット事例	・ネットで知り合った人とクラブに行ったという事例がある。 ・ネットで25歳くらいの男性と知り合って、覚せい剤を打たれたという事件があった。
実証実験を実施するための問題点の洗い出し	・すでに多くの子どもが携帯電話を持っているため、新たに仕掛けの施された携帯電話を使うようなことがあるかは疑問である。
その他	・個別に指導することはせず、全体に対してやんわりと指導する。 ・学校に連絡が来るのは、警察に補導された後、両親と連絡がつかなかった場合である。 ・塾が遅いので、11時以降に子どもが出歩いていても指導しにくい。 ・個人情報保護法の影響により、子どももアンケート等にはかなり警戒感がある。

＜現場教員ヒアリングにより把握した事項＞

IT を通して犯罪に巻き込まれた児童生徒や危険行動をとる児童生徒に関わった経験を、いずれの教員も持っていた。また、中学校段階でもすでに各学年に数名の IT を通して問題行動をとる生徒が存在すると考えられた。しかし、その割合は決して高くないので、調査

により問題児を抽出しようとするのであれば、相当数を対象に実施しなければならないと予測された。

また、学校組織や教員に児童生徒が相談する事例は、実際に発生した事故のほんの一部であり、神奈川県警によって補導された生徒が保護者の引取りがなかった、妊娠の相談から事件が明らかになった等、重篤な状態になってはじめて、教員が把握するケースが多いと考えられる。さらに指導に関しては、個別指導がしづらいために児童生徒全体に対する形式での指導を行う程度であること、家庭環境まで踏み込んでは指導ができないなどの課題も見受けられた。

さらに児童生徒の調査協力に関しては、信頼関係の構築されていないインタビュアによる聞き取り調査では、中学生が本音を言わないのではないかと考えられた。そこで，昨年度まで高校生であった大学１年生に、友人の事例としてヒアリングを行うことで有益な情報は得られないかという結論に達した。

2) 子どもへのヒアリング

a)大学生へのヒアリング

＜背景と目的＞

上記ヒアリング結果を受けて、大学生を対象に①中学校から高等学校在学時における IT の利用状況、②IT に関連した同級生の危険行動の実態や事例，③犯罪に巻き込まれるような同級生の特性、を把握することを本ヒアリングの目的とした。

＜ヒアリングの内容＞

実施日	2007年12月21日（金）
実施場所	横浜国立大学　物部研究室
対象者	横浜国立大学教育人間科学部生（2年生）　4名 ・19歳～21歳の男性2名、女性2名
インタビュア	横浜国立大学　物部、院生1名 三菱総研　　赤井

調査内容	**結果**
携帯電話、インターネットの利用状況	・携帯電話の利用は高校生時代がメインであり、大学生になった後はインターネットを主に利用する。 ・携帯電話の利用目的は主にメールであり、高校生当時１００通／日以上特定の友達とやり取りしていた。 ・大学入学後SNS（特にmixi）を利用し始める人が多く、周りの友人でも利用しているが、主には閲覧のみの利用である。
子どもの危険行動パターン	・特に女子高生では、恋人を欲しがっているが、出会う機会が少ないため、あせって出会い系サイトを利用するケースも多い。

犯罪に巻き込まれる子どもの特性	・出会い系サイトを利用する男性は、怖い感じの人、元ヤンキー、フリーターが中心である。 ・出会い系サイトを利用する女性は、自分に自信がない人、恋人と別れたばかりの人、同性の友達がいない人、彼氏がいないといられない人などである。
犯罪に巻き込まれたケース、ヒヤリハット事例	・被害状況としては、淫行条例違反、やり逃げ、売春およびその契約不履行など。
実証実験を実施するための問題点の洗い出し	ー
その他	・２～５年程度前に出会い系サイトが大流行したことがあった。

＜大学生へのヒアリングにより把握した事項＞

IT の利用状況は、携帯電話の普及率が高くなる高等学校在学時が最も頻繁であること、出会い系サイトの社会的な流行によって多くの生徒はサイトにアクセスしたことがあること、その中でも男子は、非社会的行動特性を持つ生徒、女子では対人関係に課題がある生徒が出会い系サイトにのめりこむ傾向があること、などが明らかにされた。

大まかな傾向を把握するために本ヒアリングは有効であったが、出会い系利用者からヒアリングしなければこれ以上の情報が得られないことが課題として明らかになった。この点についてはヒアリングの対象者から出会い系サイトの利用者を紹介してもらい、協力者の抽出をして努力したものの、結局当該協力者へのヒアリングの実現には至らなかった。

b)中学生へのヒアリング

＜目的＞

協力が得られ難いと考えられていた中学生に対するヒアリングであるが、総合的な学習の時間を利用した職業体験学習の一環として、調査協力の機会が得られた。そこで、①対象生徒の IT の利用状況、②IT に関連した同級生の危険行動の実態や事例，③犯罪に巻き込まれるような生徒の特性、④実証実験の可能性について、ヒアリングを行い、実態把握および実証実験の進行にかかわる問題点の洗出しをすることを、本ヒアリングの目的とした。

＜ヒアリングの内容＞

実施日	2008年02月04日（月）
実施場所	（独）情報通信研究機構小金井本部5号館
対象者	東京都多摩地区の私立中学生6名 □ 男性4名、女性2名
インタビュア	情報通信研究機構　滝澤 横浜国立大学　　物部 三菱総研　　赤井

調査内容	結果
携帯電話、インターネットの利用状況	・携帯電話は6人中5人が所有 ・内1名（女性）は小学校から所有 ・携帯電話での通話は、親との連絡やメールでは文章が長くなるときであり、それ以外は主にメールを利用する。 ・メールは主に同性同士の友人と利用する。 ・メールの内容はゲーム等、趣味の話題である。
子どもの危険行動パターン	―
犯罪に巻き込まれる子どもの特性	―
犯罪に巻き込まれたケース、ヒヤリハット事例	・女子中学生の友人に、12歳年上の男性を恋人として紹介された事例があった。 ・男子生徒では、女子生徒の友人のような例は存在しない。
実証実験を実施するための問題点の洗い出し	・できれば利用したくない。 ・何か特典（ゲームなどの提供）があれば、利用してもよい。 ・保護者や教師に連絡が行くよりは、自分に連絡してくれるほうがよい。 ・アラートが発せられて引き返すことができる子どもには、このシステムは必要ないのではないか。
その他	・「２ちゃんねる」などのメジャーな掲示板で使われている隠語については把握しているが、個人サイトなどのローカルなものについてはよくわからない。 ・中高生から隠語を教えてらおうとしても教えてくれないだろう。 ・隠語を収集するなら、直接個人サイトなどで張っている必要がある。 ・あるサイトでは、入力された単語を同じ読みで意味が異なる単語に変換する機能を持つものがある。

＜中学生へのヒアリングにより把握した事項＞

男子と女子でＩＴの利用方法が違うので、犯罪に巻き込まれるケースも異なると考えられた（男子は、ワンクリック詐欺や恐喝など、女子は売春やレイプなど）。また、実証実験のフィールドや対象として、中学生では協力が得られにくいと考えられた。また、ヒアリングでは少数事例しか抽出することができないので、アンケート調査をする必要性も認められた。

3)　中学生および高校生アンケート調査

＜目的＞

そこで、中学生および高校生を対象に①中学生高校生の IT の利用状況、②IT に関連した中学生高校生の危険行動の実態や事例，③犯罪に巻き込まれるような生徒の特性、④性格

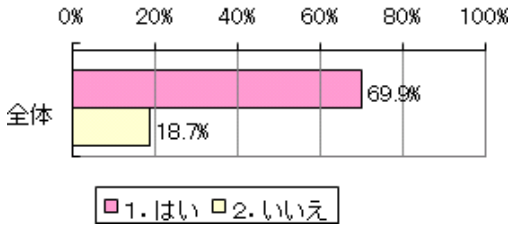
特性に関する調査を実施し、ヒアリング結果との整合性、実証実験校の可能性、仮説の妥当性について、検討することが目的である。

<アンケートの結果>

横浜市および鎌倉市の公立中学校それぞれ１校、合計２校を対象として、中学生に対するアンケートを実施し、それぞれの中学校で有効回答を 81 件と 85 件を得た。

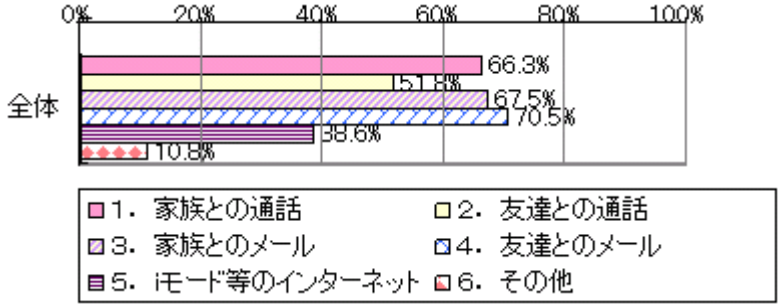
その結果の概要を以下に示す。

携帯電話の所有率



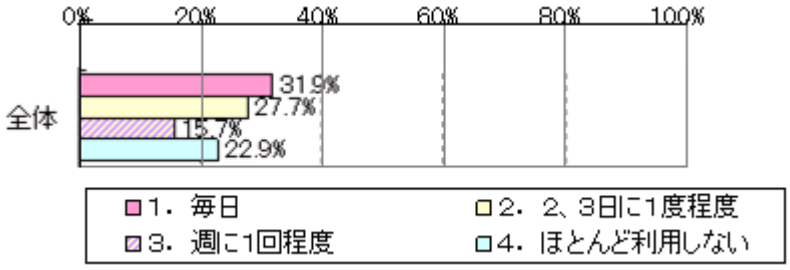
約 70%が携帯電話を有している。

携帯電話の利用目的



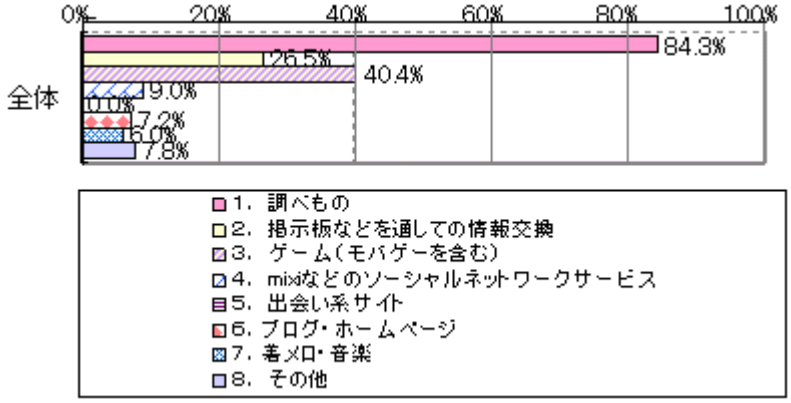
70%程度の生徒が家族との通話・メールに加え、友達との通話・メールに使う。さらには、インターネットの利用は 40%に及んでいる。

インターネット（携帯での利用を含む）の利用頻度



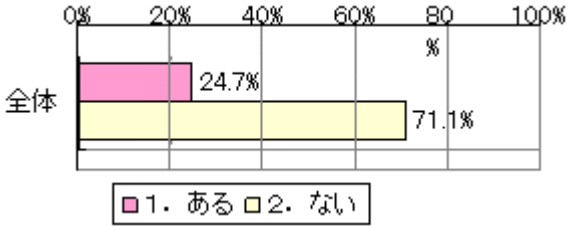
毎日利用している生徒は30%程度であるが、週に1度以上利用する生徒は70%程度となる。

インターネット（携帯での利用も含む）の利用目的



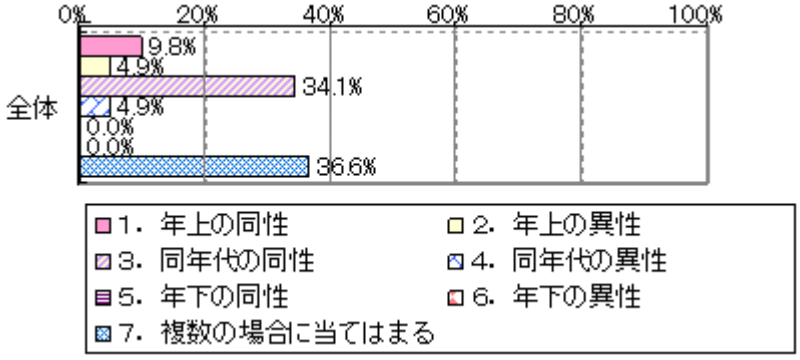
全般的には、調べものでの利用が多いが、掲示板（26.5%）、SNS（9/0%）、ブログ（7.2%）等見知らぬ人と出会う可能性のあるサイトの利用も存在する。

インターネットによる知らない人と親しくなった経験



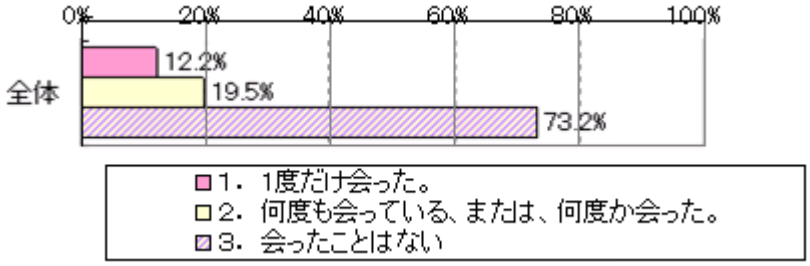
約1/4の生徒が、インターネットを通じて知らない人と親しくなったと回答している。

知り合った人の属性



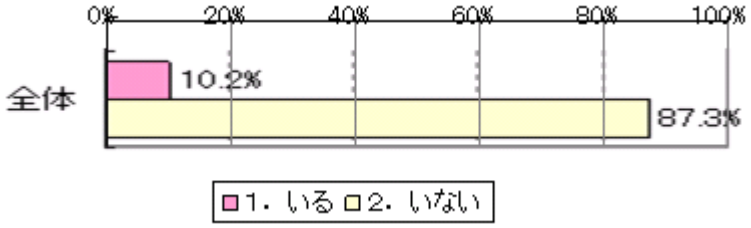
異性との出会に関しては把握できていない。年上の人と親しくなった事例は15%程度となっている。

実際の対面



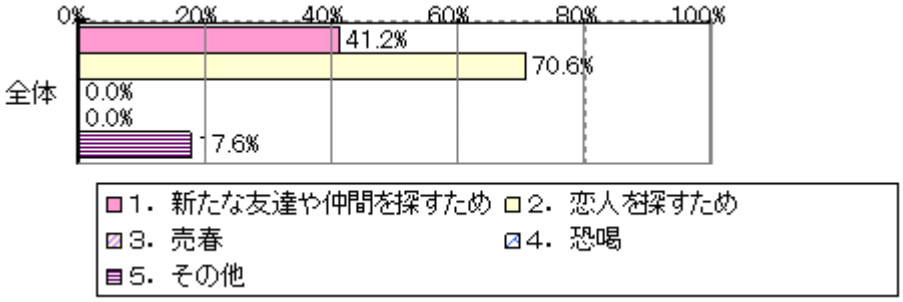
インターネットを通して、知らない人と知り合った生徒のうち、約30%が対面している。

友達の中でインターネットを用いて異性との出会いを求めている人の割合



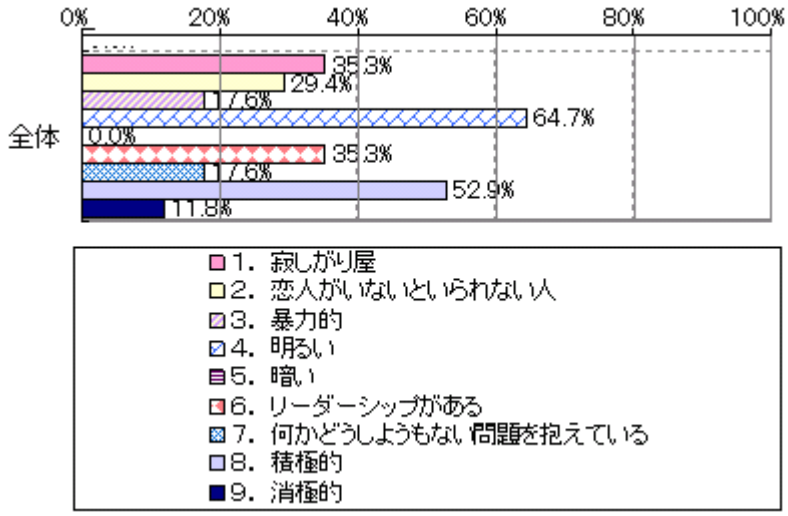
約10%の生徒が、友達のなかで異性との出会いを求めている人がいる、と答えている。

インターネットを用いて異性との出会いを求める理由



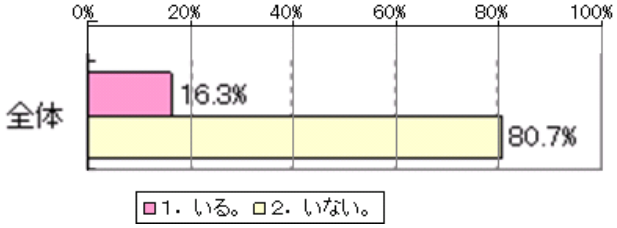
恋人を探すために、インターネットでの出会いを利用する割合が70%となっている。

インターネットを用いて出会いを求める人（友達）の性格



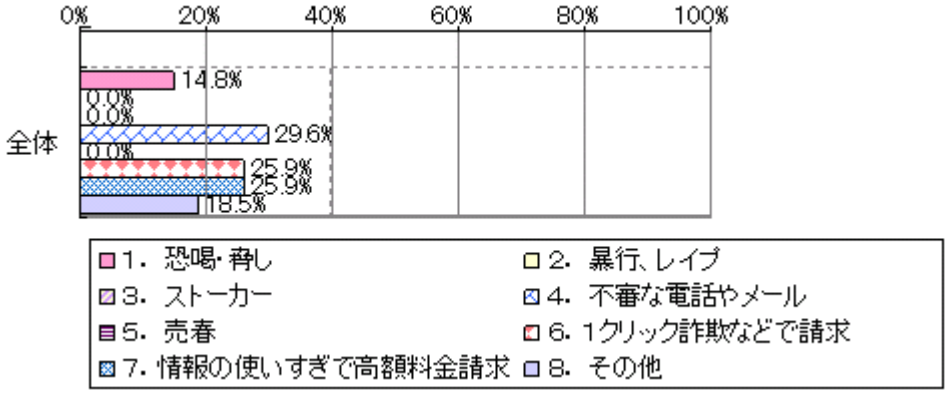
「明るい」64.7%、「リーダーシップがある」35.3%となっている。また、「寂しがり屋」35.3%、「恋人がいないといられない人」29.4%である。この設問のみでは、インターネットを用いて出会いを求める人の性格の傾向を把握することは困難である。

インターネットを通して危険な状況に陥った友達の割合



16%の生徒が、インターネットを通して危険な状況に陥った友達を知っている。

危険な状況の分類



恐喝・脅し、不審な電話やメール、ワンクリック詐欺、高額請求などに遭遇している実態が明らかになっている。

＜アンケートにより把握した事項＞

中学生に対するアンケートにより、中学生のインターネットや携帯電話の利用実態、インターネットを通した出会いや危険な状況との遭遇の実態の把握、さらには被害に遭遇する生徒の日常生活や性格との関係の把握に努めた。しかし、インターネットや携帯電話の利用実態、インターネットを通した出会いや危険な状況との遭遇の実態はある程度把握できたものの、日常生活や性格との関係の把握には至らなかった。これらは、教員や大学生、中学生のヒアリングによる補完することができたと考えている。

4）危険な状況に遭遇するに至るログに関する情報収集

インターネットおよび文献調査にて、危険な状況に遭遇するに至るログに関して収集を行い、サイバー空間における独特の言い回し、およびサイバー空間とリアル空間に跨る危険な状況に遭遇するパターンに関する検討を行った。

以下は、サイバー空間での出会いが、リアル空間における対面につながる事例である。出会い系サイトをまったく利用したことがない成人男性が、成人女性と実際に会うまでにやりとりしたメールの内容を再構成したものである。その目的は、まったく出会い系サイトを利用したことのない素人でも実際に女性と会うことができることを示すことである。なお図中の☆は男性、★は女性が送信したメール本文である。

メールの内容	コメント
★ メールありがとうございます。年上ですけど、大丈夫だったらメールください。	
☆ 変事ありがとです☆年齢は気にしてないから全然大丈夫だよ。もし平気なら携帯の方にメールもらえたら嬉しいです☆アドは＊＊＊＊＊＊です。	
★ 今手もとに携帯がないのであたしのアドレスをいれておきますね。＊＊＊＊＊＊です。名前はのりです。	携帯でのメールの送受信に移行することが重要だと考えられる。
(中略)	
以後、携帯	
(中略)	相手のことを質問して、誘う素振りを見せる。
☆ そっかあ(笑)今はどういうのが好きなのかな？	
(中略)	
☆ なるほどね。のりちゃんはどのへんに住んでるのかな？	
(中略)	
☆ ＠区なんだね。ちなみに俺は＠区だったりするんよー	
★ 近いちかいね～♪＠区のどのへん？	
(中略)	
次の日	
☆ やほ☆お疲れ様！今何してるのかな？(顔文字)	
★ 今仕事から帰ってるんだけどさむさむだな～	
☆ 大丈夫かあ？今日マジ寒いからね。もしかし薄着とか(笑)	
★ いんや～今日はダウン着てるんだけど寒いね･･･	

(中略) ☆ いやいや時間ないから自炊できないのは仕方ないよ～あっよかったら、のりちゃん写メほしいな！ぶっちゃけ好みだったからメールしたし(顔文字)お願いしまーす(顔文字) ★ こんなのしかないんだ･･･ごめんね･･･。(写メ添付) ☆ ありがとう☆うれしい～(顔文字) (中略)	写真を送るように依頼する。
☆ なるほどね！お仕事はどういうことしてるの？？ ★ あたしはアパレルの販売やってます。 (中略) ★ うん。シフトだから不定期！お風呂に入ってきまあす！ ☆ お背中お流し･･･笑。 いってらっしゃい ★ シャワーだから早いよ～♪ 顔がさむさむっ(顔文字) ☆ あっためたくなるじゃんよ(笑) ★ ありがとう☆気持ちは頂きましたぁ☆ ☆ 風邪ひかんようにおやすみ☆	以後、男が質問、女が回答のパターンが続く。 仕事を聞いて、リアルの世界に徐々に近づく。
次の次の日(前日はメールしなかった) ★ 今日はすっごい寒いね～(顔文字) NORI (中略) ☆ 俺でよけりゃのりちゃんにたくさんメールするぜ！あと遊んだりさ♪鍋だよ鍋！(笑) ★ 鍋いいね☆ (中略)	会うことを想定して、食事の話をする。
☆ 本場の味がどんなのか調べにいかない？(笑) 休みとか不規則なんだよね？ ★ うん不規則。でもシフトでて明日お休みです☆ ☆ わぁお じゃ韓国の味を調べにいこうよ！ ★ マージーですか よろしくお願いします!! (後略)	対面への誘いをする。間接的に食事に誘う。 合意成立。

上記より、以下の事項を把握した。

a) 最初から最後まで、サイバー空間の軽い（口語体の文言を用いて、決して深刻な会話はせず、当たり障りの無い話題で、顔文字や、符号を用いる等）会話を楽しんでいる
b) 男性からリアル空間の趣味や生活に関して答えやすい質問を行い、女性が答えるパターンが続く
c) 男性は当初から対面することを念頭に会話を進め、食事の話から糸口を掴んで、対面の誘いを切り出す

また、上記では、危ない状況に陥る独特の言い回しは把握できなかったが、インターネット上（援助交際掲示板を解読せよ、http://www.deaijam.com/dictionary/enjo.php）から以下に例示するような特徴的な言い回しを抽出している。

「いつも袋周辺でウリしてるョ☆1回3以上・月30以上（16♀）」
「JC、JKのみ。 ホ別フェ有ゴ有2 でサポ♪ JCなら3以上！ （49♂）」

5）まとめ

上記ヒアリングとアンケートにより、以下の事項を把握した。

- 問題を抱える子どもがサイバー空間を経て、問題を抱える大人と遭遇し、暴行、売春・買春等の犯罪行為に巻き込まれていく
- また、リアル空間での問題行動・危険行動から、問題を抱える大人と遭遇し、直接犯罪行為に巻き込まれていく場合もある。
- 問題をかかる大人との遭遇で、事件に至らなかった場合はヒヤリハット事例となる。

これらは図１のように図示できる。

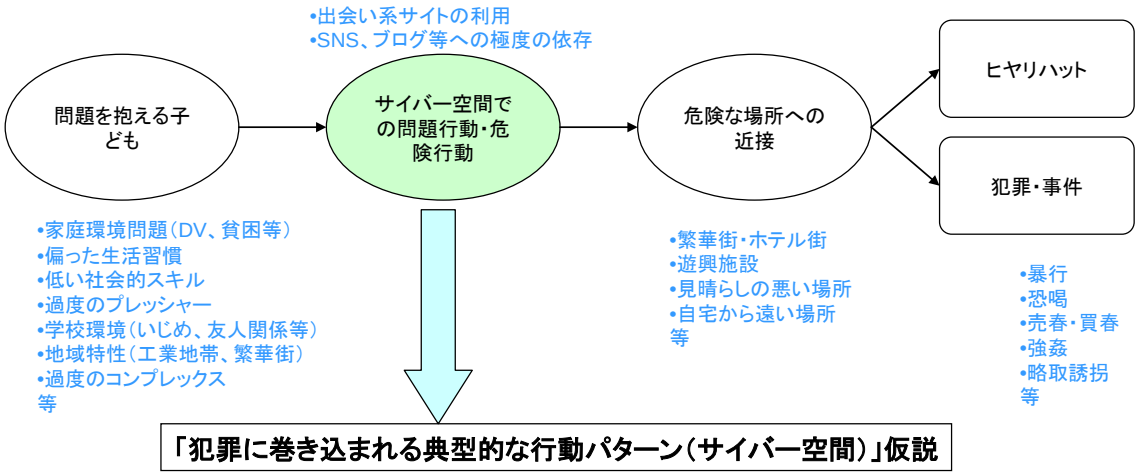


図 1　子どもが犯罪に巻き込まれるパターン

次に、ヒアリングおよびアンケートを通して、インターネットを通じて子どもが犯罪に巻き込まれるパターンを4つに分類した。そのパターンを表１に示す。これらのパターンを詳細化して、ヒヤリハットデータベースとして事例に基づくデータベースの充実を図ることにより、そのパターンに陥った子どもに対してアラートを発することが可能となる。

表 1　インターネットを通じて犯罪に巻き込まれる4つのパターン

		行動内容	事件例
利害一致型	パターン1	出会い系サイト、SNS、ブログ等で、不特定の誰かを誘うメッセージを子どもが発信し、不特定のものからのアクセスが発生する。	売春事件、買春事件の多く
	パターン2	出会い系サイト、SNS、ブログ等で、不特定の誰かが、子どもを誘うメッセージを発信しており、子どもがそれにアクセスする。	売春事件、買春事件の多く 愛知県少女殺害事件（2004.11）
共感型	パターン3	SNS、ブログ等で、子どもが記載している内容に関し、関係者とは思われない人からの、共感等を伝えるメッセージ等のアクセスが発生し、複数回のコミュニケーションが発生する。	長崎・大阪ブログ誘拐事件（2007.10）
	パターン4	SNS、ブログ等で、見知らぬ誰かが記載した内容に関し、共感等を伝えるメッセージを子どもがコメントとして記載することでアクセスが発生し、複数回のコミュニケーションが発生する。	

(2) サイバー／リアル空間モニタリング情報分析手法調査

企画調査計画書の記載内容

PCおよび携帯電話を用いて、インターネット上のサービス（SNS、出会い系等）を利用し、サイバー空間でやり取りされる情報を捕捉すると共に、携帯電話の位置検索サービスから取得できる位置情報を利用し、具体的な危険パターンの導出を行う。また、導出された危険パターンを自動的に検出するためのアルゴリズムの検討を、データマイニング、推論等のアルゴリズムの調査を行った上で検討する。なお、サイバー空間モニタリングでは、実際にPC、携帯電話からサービスやメール等を利用することで一次情報を取得し、リアル空間モニタリングでは携帯電話の位置検索サービスを利用することで位置情報を得ることとする。

具体的な作業項目は以下のとおりである。

【作業項目】

- PC、携帯電話を用いた実際のサイバー空間モニタリング情報収集に関する調査
  - PC3台および携帯電話3台を利用してSNS、出会い系、掲示板等のインターネットサービスを利用し、ログを収集し、犯罪に巻き込まれるパターンを抽出する。
- 携帯電話を用いたリアル空間モニタリング情報収集に関する調査
  - 携帯電話における位置検索サービス（例えばNTTドコモ　イマドコサーチ等）を利用することを通して、子どもの位置検索情報を収集する技術を調査する。
- 推論およびデータマイニング手法の調査
  - ベイズ推論等の推論手法、データマイニングおよびストリームマイニング技術、メッセージ解析等の技術を調査する。
- サイバー／リアル空間モニタリング情報分析手法の検討
  - 上記の調査内容から自動的に危険パターンを抽出し、関係者にアラートを発する方法に関して検討する。

本節では、「携帯電話を用いたリアル空間モニタリング情報収集に関する調査」、「推論およびデータマイニング手法の調査」、「サイバー／リアル空間モニタリング情報分析手法の検討」の作業を通して、サイバー空間（SNS、ブログ、電子メール、電子掲示板等）とリアル空間のモニタリングを実施し、それらのモニタリング結果を有機的に統合することにより、適切なタイミングで子どもにアラートを発する機能を有するシステム構築を行うための検討の成果を述べる。

なお、企画調査計画書の記載項目のうち、PC3台および携帯3台を利用したログの収集は実施しなかった。これは以下の理由による。

- (1)で示したヒアリング、アンケート、文献調査により、実態を十分に把握できたため
- ブログやSNSにて情報収集する際に、何らかの「なりすまし」が必要となるが、研究倫理上の問題があると認識したため

1) システムの全体像

ITを用いた子どもの安全確保システムの全体像は、図２の通りである。

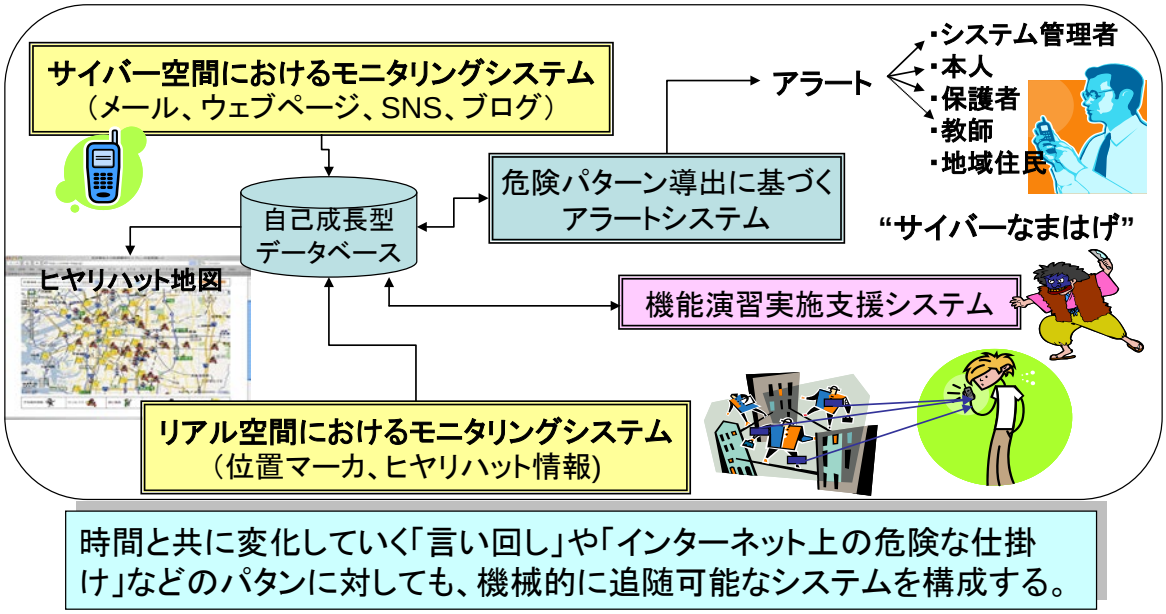


図 2 ITを用いた子どもの安全確保システムの全体像

以下では、図２の主要部分につき詳細に説明する。

2) サイバー空間におけるモニタリングシステム

サイバー空間におけるモニタリングシステムの全体像を、図 3に示す。

サイバー空間モニタリングシステムは、携帯電話上で、メール、ウェブ頁、SNS、ブログ等を常時モニタリングし、受発信パケット（以下ではこれをメッセージと呼ぶ）を抽出する。抽出したメッセージに関して、言い回しデータベースや相手先データベースを参照して、メッセージ毎の危険度を算出する。さらには、メッセージ毎の危険度を時系列にプロットし、危険度の変異をモニタリングし、ベイズ推論等により各個人のサイバー空間における危険度を算出する機能を有する。

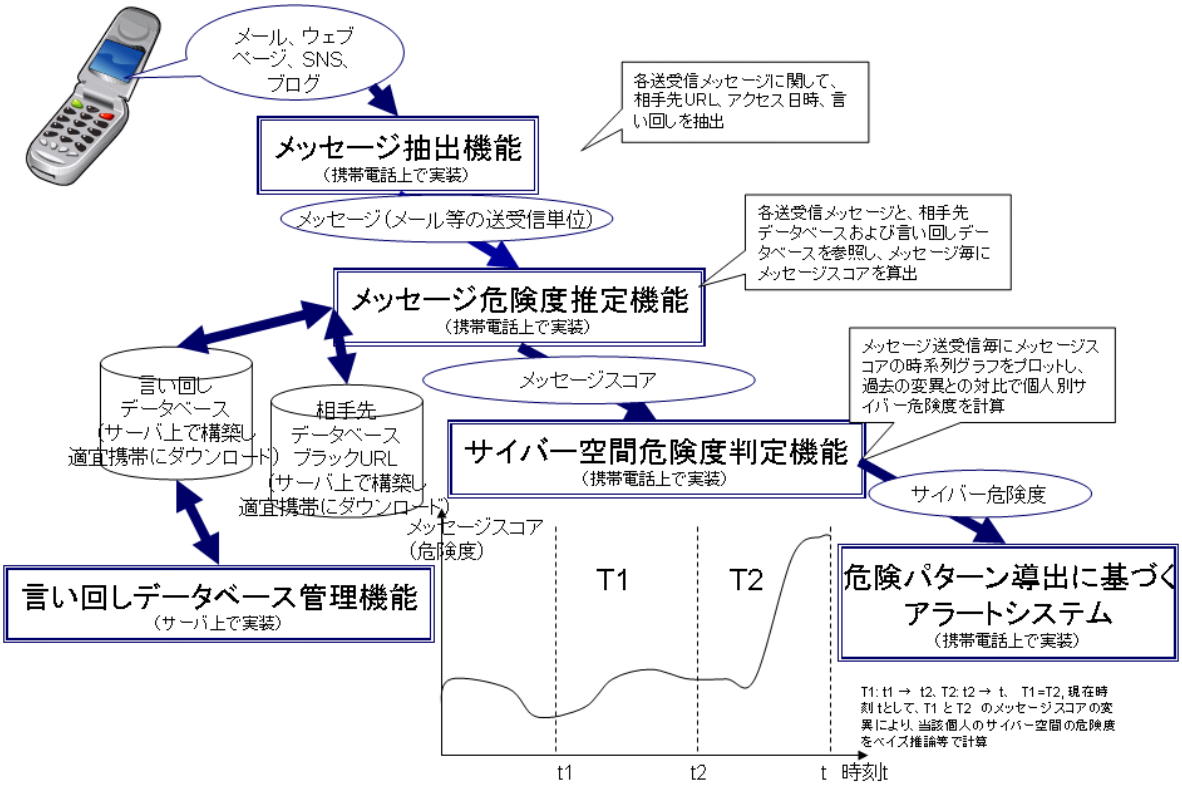


図 3　サイバー空間モニタリングシステムの全体像

i)　メッセージ抽出機能

各送受信メッセージに関して、相手先URL、アクセス日時、言い回し等を抽出する。メッセージ抽出機能は、携帯電話上で稼動することを想定している。

ii)　メッセージ危険度推定機能

各メッセージに関して、相手先データベースと言い回しデータベースを参照して、メッセージ毎に危険度を計算する（以後、メッセージ毎の危険度をメッセージスコアと呼ぶ）。メッセージ抽出機能は、携帯電話上

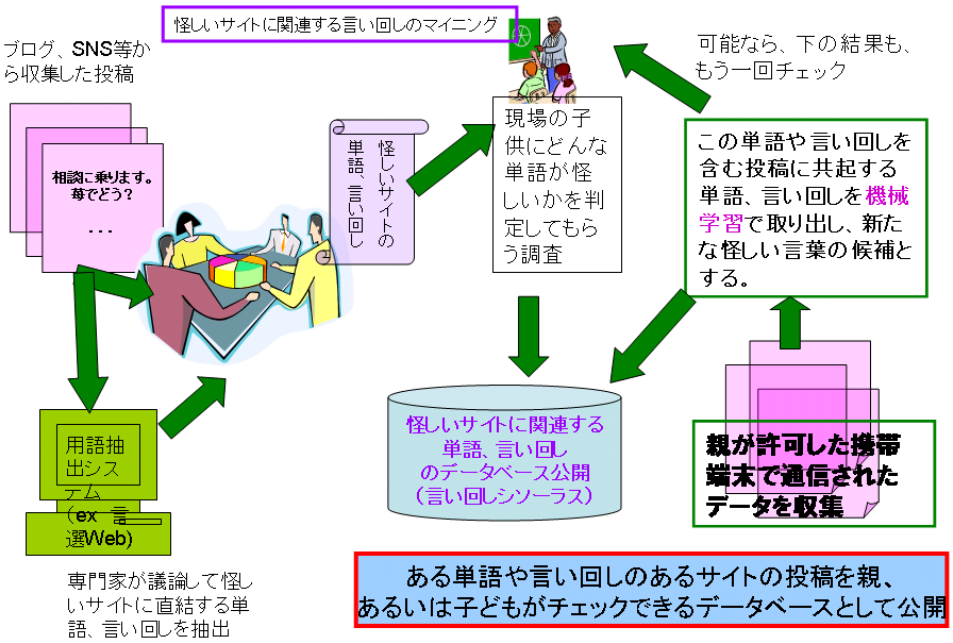
で稼動することを想定している。

iii)　**サイバー空間危険度判定機能**

各メッセージスコアを時系列に管理し、直近の1日または1週間のメッセージスコアの時系列グラフに関して、それ以前の時系列グラフと比較する。具体的には、各期間のメッセージスコアの変異を計算し、その変異の大きさをベイズ推論等により計算し、サイバー空間での危険度（以後、サイバー危険度と呼ぶ）を求める。メッセージ抽出機能は、携帯電話上で稼動することを想定している。

iv)　**言い回しデータベース管理機能**

言い回しデータベース管理機能の全体像を図４に示す。言い回しデータベース管理機能は、サーバ上で動作することを想定している。



a)　リアル空間におけるモニタリングシステム
b)　自己成長型データベース
c)　危険パターン導出に基づくアラートシステム
d)　機能演習実施支援システム

図 4　危険なサイトに関連言い回しデータベース管理機能の全体像

図４の左半分に記載されている、この専門家の分析においては用語抽出システムなどの既存システムあるいはその改善を行い利用できる。たとえば、用語抽出システムとしては、調査グループのメンバが開発した言選Web：
http://gensen.dl.itc.u-tokyo.ac.jp/gensenweb.html　が有力な候補である。

一方、図４の右半分に記載された怪しいサイトに関連する言い回しや単語の抽出処理については機械学習を援用する。

言い回しの機械学習

〈機械学習の全体像〉

今回の危険事例調査で得られたメールテキストを調べると隠語や非文法的な言い回しが散見される一方、誘いに特有の会話の流れが見られる。このようなテキストを親の承諾の元で子供に持たせている携帯端末のメールのやり取りで抽出する、あるいはアクセスしている危険サイトから送られるテキストの分析を通じて発見できれば、早期の警告を出せる。危険サイトかどうかは予め分からないことも多いので、むしろ、メールなどでやり取りされているテキストを処理して危険予知することが重要となる。

〈テキストマイニング〉

そのための技術としては、機械学習を活用するテキストマイニング技術によって、危険信号となる言い回しや単語のデータベースを構築することが有望である。ただし、どのような言い回しや単語が危険信号であるかを予め網羅することはできない。つまり、機械学習における正例（教師データ）は網羅性良く得られない。ただし、専門家の分析により少数であれば危険信号となる言い回しや単語は得られる。よって、正例と負例から識別器を構成する通常の機械学習ではなく、少ない教師データから大量の生テキスト（未分類のテキスト）を処理して教師データを拡大する半教師あり学習、場合によっては教師なし学習のアルゴリズムを開発する必要がある。テキストを対象にする半教師あり学習、教師なし学習は最近発展が著しい分野であり、本研究への寄与が期待できる。

〈チャレンジすべき問題〉

対象とするテキストは、通常の形態素解析で正確な解析ができる保証はないが、問題となる単語の多くは未知語として認識されるので、未知語に狙いを絞って機械学習を適用する方法が考えられる。一方、やや長い会話シーケンスは、マイニング処理が難しいが、言い回しシーケンスを機械学習することはまったく不可能というわけではない。ある程度の網羅性でよければ危険信号となるパタンを抽出できるであろう。

〈負例の収集〉

機械学習では負例も必要である。すなわち、上記の携帯電話のメールのやり取りで抽出できるテキストは正例であり、通常のメールのやり取りなどを負例として収集する必要がある。ただし、これは一般のメールや商品広告サイトなどを利用できるので正例よりも容易に多数収集できる。

時間的な言い回しの変化の追跡

多くの新語が生まれ廃れていることからの分かるように言語の変化は速い。特に、本研究で対象にしている危険と隣り合わせの世界では、仲間内でのみ通用する言い回しや単語があり、それらが時間とともに変容していく速度は一般の言い回しや単語より速い可能性が高い。よって、こういった時間変化に機械的に追従する技術が重要である。このような

方向性を持つ技術としてTDT(Topic Detection and Tracking)が数年前より研究されおり、その成果は参考になる。ただし、表現の種類が多いことを考えると、より高度な手法が必要になるであろう。このような手法の候補としてはベイズ統計を基礎とするLDA(Latent Dirichlet Allocation: 後述）やHDP(階層型ディリクレ過程: 後述）が有力な候補であろう。これらを時間変化データに適用することは、基礎理論的にもチャレンジングな研究テーマである。

ここで、LDAとHDPに関して補足説明を行う。

LDA：与えられたテキストコーパスの文書分類を行う。単語分布にはディリクレ分布（多項分布に類似した分布）を用いる。LDAの特徴は、文書を単一のトピックに分類を行うわけではない点にある。LDAではトピックは明示されていない潜在変数であり、文書は複数のトピックを持っても良い。つまり、いわゆるソフトクラスタリングを行う。分類される各トピックを特徴付ける単語も同時に取り出せる。つまり、単語と文書（＝複数のトピック）の両方を同時に分類できる。よって、危険なメッセージを金銭目的、裏サイトなどのカテゴリ分けを行うと同時に、それらのサイトに特有の単語を取り出せる可能性がある。ただし、現在の技術では単語単位での処理しかできない。よって、言い回しや会話シーケンスに対象を拡大するためには、テキスト処理、特に学習で利用するfeatureを検討し、抽出する手法の開発、評価実験が必要となる。

HDP：LDAは分類のカテゴリが予め与えられているが、HDPの場合は、上位の階層で無限の可能トピックを設定し、その中からデータに沿ってトピックを抽出するプロセスがあり、下位の階層では、選出されたトピックに沿って分類を行う。よって、新規なトピックに追従できる可能性がある。これを応用すると、使われる言い回しや単語の時間的変化、およびその背後にあるサイトの集合や勧誘の新規手口を早期に発見できる可能性を持つ。ただし、これは実現するためには複雑な数理モデルとfeature選択、綿密な評価実験を行う必要があり、チャレンジングなテーマである。

<u>言い回しデータベースの公開</u>

- 親の許諾の元に使っている携帯端末において、このデータベースに格納されているデータと一致するテキストが存在するかどうかを調べれば、早期の注意喚起を促すという、本研究の主目的における必須データを提供できる。
- 一方、親の許諾のもとに使っている携帯端末を持つ実験に参加していない人々も、小耳に挟んだような言い回しが危険信号かどうかを、このデータベースを検索すればチェックできる。この意味で、このデータベースは公共性の高い言い回し検索エンジンという位置づけができる。

このような活用を考えると、本研究の成果となるであろう上記データベースは公共性高い社会資産として期待できる。

3) リアル空間におけるモニタリングシステム

リアル空間におけるモニタリングシステムの機能概要を、図５に示す。

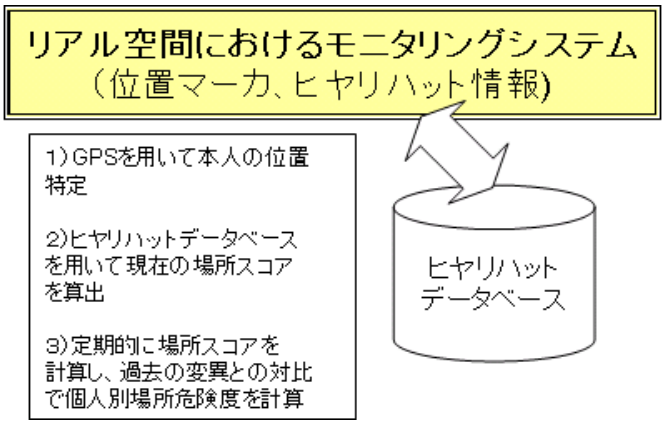


図 5　リアル空間におけるモニタリングシステムの全体像

リアル空間におけるモニタリングシステムは、携帯電話のGPS機能による位置特定、またはRFIDを用いた位置マーカによる位置特定機能を実装することにより、携帯電話を持つ子どもの現在位置をシステムがリアルタイムで取得可能とする。

さらに、そうして獲得した本人の位置に関して、予め準備されたヒヤリハットデータベースを用いて現在の場所スコアを算出する。この場所スコアは、蓄積され、時系列で管理される。時系列の場所スコアに関して、過去の変異との対比で場所の危険度（以後、場所危険度と呼ぶ）を計算する機能を有する。

なお、ヒアリヤットデータベースには、過去に子どもが危険な状況に遭遇した事例および実際に犯罪に遭遇した事例に関して、以下の情報を有するものとする。

- 危険な状況と犯罪に遭遇するパターン（表１参照）
- 各パターンにおける場所情報
- 各パターンの時刻
- 地図情報
- 地図情報とパターンとのリンク

4) 危険パターン導出に基づくアラートシステム

危険パターン導出に基づくアラートシステムの機能概要は、図６に示す。

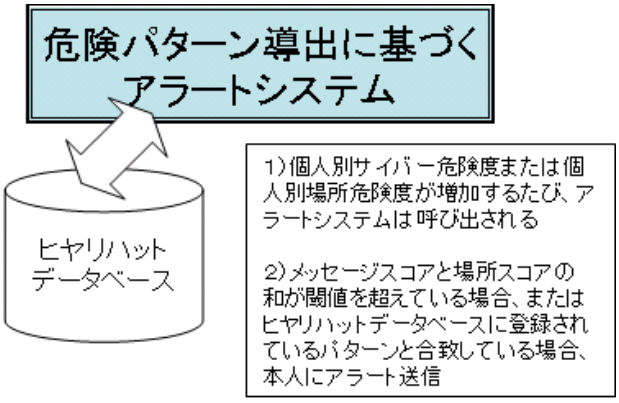


図 6　危険パターン導出に基づくアラートシステム

本システムにおいては、各個人毎にサイバー危険度または場所危険度が増加する度に、サイバー空間におけるモニタリングシステムまたはリアル空間におけるモニタリングシステムから呼び出される。

そして、サイバー危険度と場所危険度の和が、予め設定した閾値を超えている場合、子ども自身にアラートを発する。さらには、ヒヤリハットデータベースにアクセスし、そこに登録されている危険パターン（過去に子どもが遭遇した危険なパターン）と類似度を計算し、閾値を超えている場合、子ども自身にアラートを発する。

5) システムの利用法、利点、およびビジネスへの展開

a）システムの利用法

提案システムは、子ども自身が実際の危険に遭遇しないように利用することを目的としている。そのため、子どもが了承した上で、本システムを実装した携帯電話を利用し、アラートを子ども自身が受け取る仕組みを実装することを想定している。

b）システムの利点

フィルタリングはサイバー空間の入り口での対策であり、提案システムは実際の危険の間際でアラートを発し、未然に防ぐことができる。また、ブラックリスト／ホワイトリストでは対応できない部分についても対応することが可能であり、特に、頻繁にURLが変わる危険サイトへの対応、必ずしも危険サイトとは言い切れない場合への対応（SNS等）などが可能となる。

c）ビジネスへの展開

ビジネスへの展開に関して、以下の点に留意し進展を図ることができる。

- ビジネスサイドとしては、モデルに近い子どもに資源を集中的に割り当てることができ効率的である。
- また、得られた知見等を基に教材（e-learning）などを展開することが可能である。
- 保護者サイドとしては、子どもに対する抑止効果を期待できると共に、もしものときにも対応できる可能性がある。
- 子どもサイドとしては、もしものときの危険な状況に誰かが助けてくれる可能性が高くなる。

6） 附録：フィルタリングサービス、フィルタリングソフトウェアの現状調査

総務省は、2007年12月、青少年が使用する携帯電話・PHSにおける有害サイトアクセス制限サービス（フィルタリングサービス）の導入促進を図るため、携帯電話・PHS事業者（株式会社エヌ・ティ・ティ・ドコモ、KDDI株式会社、ソフトバンクモバイル株式会社、株式会社ウィルコム）及び社団法人電気通信事業者協会に対し、その取組を強化するよう要請した（総務省Webページ http://www.soumu.go.jp/s-news/2007/071210_4.html）。これに応え、各通信事業者はフィルタリングサービス事業者のサービスを利用する形で、有害サイトアクセス制限の導入を進めている。本企画調査の一環として、フィルタリングの技術的な面に関して調査を行った。これは、本企画調査で提案するモニタリングとのフィルタリングの関係を明らかにするためである。

a)フィルタリングURLを作成している主な企業

ネットスター株式会社　http://www.netstar-inc.com/

アルプスシステムインテグレーション株式会社（ALSI）とトレンドマイクロ株式会社による共同出資で2001年に設立されたネットスター株式会社は、フィルタリング用のURLリストの作成を主な業務とし、現在、NTTドコモ、KDDI、ソフトバンク、ウィルコムの4つの通信事業者によるフィルタリングサービスで用いられるブラックリストを作成している。ネットスター株式会社のWebページによれば、約35人のスタッフが目視でサイトを分類しているとのことである。ブラックリストを作成する以外には、URLリストやその情報を読み取るミドルウェアや連携開発用の情報をパートナーに提供するなどの業務を行っている。同社のブラックリストを採用しているパッケージソフトウェアには、アルプスシステムインテグレーション株式会社のInterSafe、トレンドマイクロ株式会社のInterScan WebManager、サイバーリンクトランスデジタル株式会社のグーイファミリースタイルなどがある。ネットスター株式会社のWebページによると同社は国内のURLフィルタリングリストでトップのシェアを有しているとのことである。

デジタルアーツ株式会社　http://www.daj.jp/filter/db.htm

ネットスター株式会社以外にはフィルタリングソフト「i-フィルター-5」を販売してい

るデジタルアーツ株式会社のように、独自にURLリストのデータベースを作っているところもある。また，デジタルアーツ社が全ての株を持っている株式会社アイキュエス社（http://www.iqs-j.com/ ）が販売しているソフトウェアのCyber sitterや、サーバにインストールするソフトウェアであるAD-Guard、オンラインのフィルタリングサービス親子ネットは、デジタルアーツ社のURLリストを適用している.

b)　携帯電話のフィルタリング機能について

携帯電話でのフィルタリングによるアクセス制限サービス

現在（2008年3月）実施されている携帯電話向けのフィルタリングサービスを通信事業者毎に分類すると以下のように整理できる。

NTTドコモによって提供されているフィルタリングサービスはアクセス制限機能と呼ばれ、キッズiモードフィルタ、iモードフィルタ、時間制限の３つがある（http://www.nttdocomo.co.jp/service/site_access/access_limit/）キッズiモードフィルタはiモードメニューサイトの中でもグラビアやコミュニティカテゴリに属さないサイトのみが閲覧可能で、一般サイトは閲覧できない。iモードフィルタは、キッズiモードサイトで閲覧可能なサイトに加え、一般サイトの中でも有害とされているURLリストに含まれるサイトが閲覧できない。これらのフィルタに加え、夜間(22時)から早朝(6時)まで、iモードを使った、全てのサイトへのアクセスを制限する、時間制限サービスがある。時間制限サービスは、残りの2つのサービスと併用できる。

KDDIによって提供されているフィルタリングサービスはEZweb利用制限とEZ安心アクセスサービスがある（http://www.au.kddi.com/ezweb/service/anshin_access/index.html）。EZweb利用制限は、料金照会やauホームページのみ閲覧可能で、出会い系サイトや成人向けサイトなどが存在する一般サイトへのアクセスが一律規制される。EZ安心アクセスサービスには、接続先限定コースと、特定カテゴリ制限コースの2つがある。接続先限定コースは、KDDI基準を満たしたサイトのみ閲覧が可能で、KDDI基準を満たしていないサイトの閲覧は不可となる。特定カテゴリ制限コースは、ネットスター株式会社により提供されたURLデータベースに登録されているURLの中で、特定カテゴリに登録されているサイトの閲覧ができず、それ以外の一般サイトは閲覧が可能となる。

ソフトバンクによって提供されているフィルタリングサービスは、Yahoo!きっずとウェブ利用制限、インターネットアクセス制限の3つがある（http://mb.softbank.jp/mb/support/safety/web/for_kids.html ）。Yahoo!きっずは、あらかじめソフトバンクが登録したサイトのみにアクセスできる、子供向けコンテンツを中心としたサービスである。ウェブ利用制限は、ネットスター株式会社の基準に基づき、ソフトバンクオフィシャルサイトの一部と一般サイトの一部の閲覧が制限される。インターネットアクセス制限は、URLの直接入力によるインターネットアクセスおよび、URLリンク付きメールからのインターネットアクセスを防止することができる。携帯電話から直接

設定する。

ウィルコムによって提供されているフィルタリングサービスには、有害サイトアクセス制限サービスがある（http://www.willcom-inc.com/ja/service/filtering/index.html）。ネットスター株式会社の基準に基づき、特定のカテゴリに該当したサイトの閲覧が制限される。

URLリストを利用した迷惑メール対策サービス

ソフトバンクとNTTドコモはネットスターのURLリストを利用して、メール本文中にURLリストデータベースにあるURLがあった場合にそのメールを携帯電話に配信しないという迷惑メール対策サービスを行っている。ソフトバンクモバイルでのサービス名はURLリンク付きメール拒否設定、NTTドコモでのサービス名はURL付きメール拒否設定と、それぞれ名づけられている（http://www.nttdocomo.co.jp/info/spam_mail/measure/url/index.html、http://mb.softbank.jp/mb/support/3G/mail/original_mail/url.html）。

c）パソコン向けの主なフィルタリングソフトウェアの機能について

市場に流通しているフィルタリングソフトウェアは、サーバにインストールして複数のクライアントのウェブへのアクセスをフィルタリングすることを目的としたソフトウェアや、親が特定のパソコンにインストールすることでそのパソコンを利用した子どものウェブへのアクセスをフィルタリングすることを目的としたソフトウェアなどがある。ここでは後者のソフトウェアに関して、日本国内で流通しており、主な企業のブラックリストを採用しているソフトウェア４つについて、それらが持つ主要な機能を調査した。結果を表２にまとめる。

表２　パソコン用フィルタリングソフトウェアの機能

製品名	販売元	主な機能
Windows Live OneCare Family Safety	マイクロソフト株式会社	・ユーザごとにフィルタリングルールを決めることができる ・有害なサイトは複数のカテゴリに分類されており、どれにアクセスできないようにするか設定できる ・特定のサイトをホワイトリストに入れてアクセス可能にできる ・コミュニケーションツールの利用や，連絡相手を確認・制限できる ・フィルタリングルールに従い検索エンジンの結果表示をブロックできる ・フィルタリングルールによってアクセスできない場合、子どもから親にアクセス許可をリクエストできる
グーイファミリースタイル	サイバーリンク トランスデジタル株式会社	・ユーザごとにフィルタリングルールやウェブ閲覧のスケジュールを決めることができる ・有害なサイトは複数のカテゴリに分類されており、どれにアクセスできないようにするか設定できる ・特定のサイトをホワイトリストに入れてアクセス可能にできる ・ユーザごとに、いつ、どのサイトを閲覧したかのようなアクセス履歴を確認できる
i-フィルター5.0	デジタルアーツ株式会社	・ユーザごとにフィルタリングルールやウェブ閲覧のスケジュールを決めることができる ・有害なサイトは複数のカテゴリに分類されており、どれにアクセスできないようにするか設定できる ・ユーザごとに、いつ、どのサイトを閲覧したかのようなアクセス履歴を確認できる ・特定のサイトをホワイトリストに入れてアクセス可能にできる ・閲覧可能な掲示板やチャット・ブログなどへの書き込みを禁止できる ・フィルタリングルールに従い検索エンジンの結果表示をブロックできる ・事前に登録された単語を伏字表示できる
ウィルスバスター2008	トレンドマイクロ株式会社	・有害なサイトは複数のカテゴリに分類されており、どれにアクセスできないようにするか設定できる ・あらかじめ氏名，クレジットカード番号などの個人情報を登録し、ウェブブラウザ，メール，インスタントメッセンジャによる許可されていないサイトへの情報流出をブロックできる

(3) 実証実験の体制検討

企画調査計画書の記載内容

システムの有効性を検証する実証実験について、実証実験フィールドおよび関係者への調整等につき調査・調整を行う。作業項目としては、以下を想定する。

【作業項目】

- 実証実験フィールドの選定
  - 上記２．１の調査結果を基に選定する。特にPC・インターネットの使用率が高く、トラブル事例の多い小学校または中学校を選定する。
- インターネットサービス事業者および通信事業者の選定
  - 実証実験フィールドとして選定した小学校または中学校の児童または生徒がよく利用するSNS等のサービス事業者を選定する。
- 実証実験実施にあたっての課題抽出と解決法の検討
  - 実証実験実施に向けての保護者・教員等への説明方法と協力要請について検討する。
  - 被験者となる子どもへの実証実験への協力を促進する方法について検討する。
  - 実験実施上課題となる子どものプライバシー確保を中心とした人権への配慮方法について検討する。

1) 実証実験フィールドに関する検討

実証実験に関しては、本調査にてヒアリングおよびアンケート協力先の中学校および高等学校に関して、実証実験協力に関して合意を得ており、実証実験対象として有望である。実証実験の体制は、以下のように想定している。

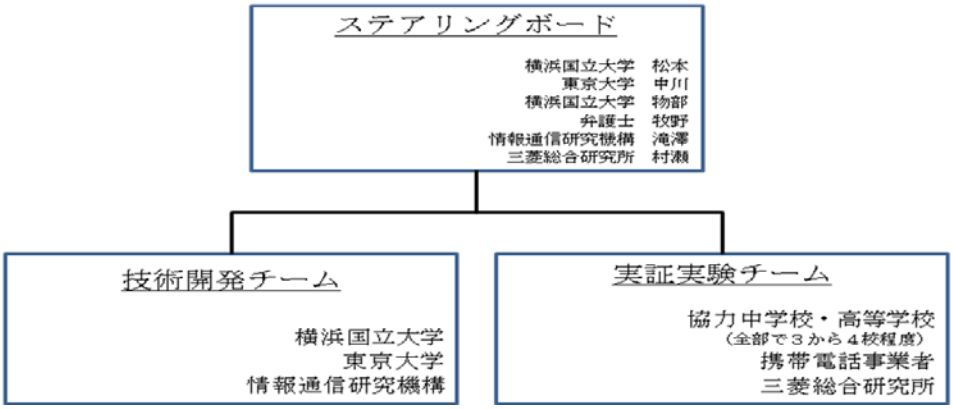


図 7　実証実験の体制

2) インターネットサービス事業者と通信事業者に関する検討

本実証実験に際しては、携帯電話事業者との協力の下に、携帯電話上で稼動可能なアプリケーションを製作・実装することが不可欠である。この点に関して検討を進めた結果、本調査研究の一員である独立行政法人情報通信研究機構は、某携帯電話事業者（以下携帯電話事業者）のモバイルソリューションパートナーとなっており、この携帯電話における

アプリケーション開発と実装の権利を得ていることが判明し、実証実験実子のためのアプリケーション開発および実装、さらには運用に問題はないことが分かった。

3）課題の抽出

実証実験を行うに際し、想定される法的な課題に関して検討を行った。携帯電話を用いた実証実験に関して、当初、親の了解を得るのみで、子どもに携帯電話を貸し出す方式を検討し、以下の問題設定の下に、弁護士とのディスカッションを通じて検討した。

> 問題設定
> 「子どもが利用する携帯電話に関して、親が了解していれば、通信の秘密の侵害に係る問題はないか。」

弁護士を含めた検討の結果、以下の結論を得た。

○サービスとして提供する場合

- 携帯電話に関する契約が、親と携帯電話事業者の間で行われれば、子どもの通信内容を収集することに関する契約上の問題はない
- 契約者が親権を有している点からしても法的問題はない
- 子どもは未成熟であっても個人であるため、基本的には告知を行った方がよい

○実証実験として携帯電話を提供する場合

- 子どもにも実証実験であることを認識してもらう必要があり、子どもの同意書が必要ではないか
- 「サイバーなまはげ」に関しては、子どもの心理的プレッシャーに配慮して、子どもが混乱を生じないような仕組みを設置しておくことが重要

> 問題設定
> 「実証実験する際に、システムの構築・運用に際して問題がないか。」

弁護士を含めた検討の結果、以下の結論を得た。

○言い回しデータベースに係る問題

- サーチロボットがウェブページをクローリングする際に、ウェブページを電子的にサーバにコピーする行為は、現状の著作権法違反である可能性が高い
- しかし、サーチエンジンの公共性に鑑みて、ウェブページを蓄積したデータベースを公開する行為が伴っていれば、次回の著作権法改正時に適法となる可能性もある

○モニタリングに係る問題

- 携帯電話の所有者である親および利用者である子どもの了解を得て、通信のモニタリングを行った場合でも、相手方の了解を得ていないという問題が残る
- そのため、通信のモニタリングを行うのではなく、携帯電話上で稼動するシステムを構築し、通信時ではなく、携帯電話での入力および出力上にモニタリングを行うシステムが望ましい

(4) まとめ

本調査では、ITを用いた子どもの安全確保システム全体像を明らかにし、システム構築と実証実験を行うに際しての課題についても検討を行った。その結果、図８に示すITを用いた子どもの安全確保システムが有用であるとの結論を得た。

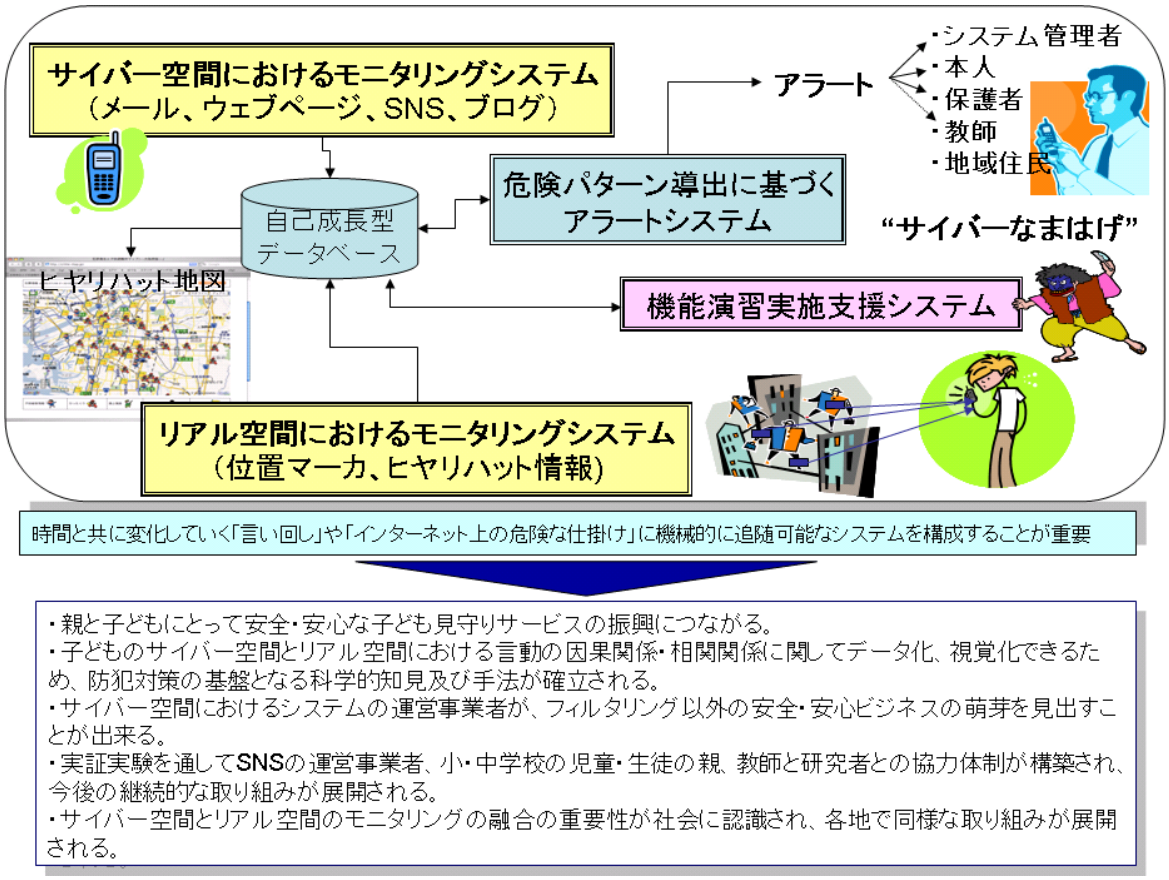


図 8　ITを用いた子どもの安全確保システムの全体像と効果

なお、本研究開発は、子どもの安全確保のための他の取り組みとは以下の点で異なる。

a) GPS等により子どもの現在位置を把握し、親に通知するシステムは、現在位置だけをモニタリングするため、それまでの行動の経緯が把握できず、小学生には有用であるものの繁華街等に行く機会も増える中高生には有用ではない。

b) サイバー空間における子どもの安全確保の取り組みは、フィルタリングソフトの導入が中心となっているが、安易なフィルタリングソフトの導入は子どもの健全なコミュニケーションの機会を奪うことにつながり、安全確保には至らない可能性がある（石野純也:「ケータイチルドレン」, ソフトバンク新書, 2008年3月参照）

c) 上記a)およびb)を勘案し、フィルタリングソフトに依存せず、子どものサイバー空間

とリアル空間での行動を適度にモニタリングし、子ども自身にアラートを発するシステムを実装すれば、保護者、教師、子ども、その他関係者にとって非常に有用である

また、課題を以下のように整理した。

a) 危険パターンの詳細化
子どもがインターネットを通した危険に陥るパターンに関して、今後もさらなる情報収集を進め、詳細化が必要である。

b) 実証実験の詳細設計
実証実験に際しては、携帯電話の配布台数、その際の情報開示の方法、実証実験フィールド、配布期間、評価方法等に係るさらに詳細な検討が必要である。

上記を念頭において、平成20年度応募に向けたプロジェクト提案書作成を行っている。

(5) その他

本企画調査に係る研究者の主なミーティングの実施状況を以下に示す。

第1回						
日　時	2007年9月28日（金）19:00-21:10			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 富井 遠山	滝澤 吉岡 薗田 中里	中川	村瀬 牧野 佐藤 赤井	増田	
議　事	1）企画調査計画書の審議					

第2回						
日　時	2007年10月11日（木）10:30-12:00			場　所：横浜国立大学		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 遠山	滝澤 吉岡 薗田 中里		村瀬 佐藤 赤井		
議　事	1）企画調査採択プロジェクトの代表者説明会での注意事項を確認 2）調査の全体方針について議論 3）ヒアリング、アンケートの方針について議論					

第3回						
日　時	2007年11月06日（火）19:00-22:20			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 遠山	滝澤 吉岡 中里	中川	村瀬 佐藤 赤井		
議　事	1）子どもの危険の実態把握方法に関し議論					

第4回						
日　時	2007年12月03日（月）18:00-21:10			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 吉岡 遠山	滝澤 井上 薗田 中里	中川	村瀬 赤井	増田	
議　事	1）携帯電話を含む子どものインターネット利用状況と危険事例調査の結果について検討 2）法律上の問題に関して法律家と相談することを決定					

第5回						
日　時	2007年1月09日（水）18:30-21:55			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 吉岡 遠山	滝澤 井上 薗田 中里	中川	村瀬 牧野 佐藤 赤井	増田	
議　事	1）大学生へのヒアリングの結果につきて確認 2）企画調査の中間報告会に向けての準備の検討					

第6回						
日　時	2007年2月27日（水）18:30-21:20			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 吉岡 遠山	井上 薗田 中里	中川	村瀬 佐藤 赤井	増田	牧野弁護士
議　事	1）子どものインターネット利用状況と危険事例調査の結果を確認 2）インターネットを通じての出会いとメッセージ交換事例につき議論 3）システム開発と運用に係る法律上の問題につき議論					

第7回						
日　時	2007年3月28日（金）18:55-22:34			場　所：大手町		
参加者	横浜国立大学	情報通信研究機構	東京大学	三菱総合研究所	東京電機大学	その他
	松本 物部 富井 遠山	滝澤 薗田 中里	中川	村瀬 赤井	増田	牧野弁護士
議　事	1）法律上の課題につき議論 2）実証実験の体制につき議論 3）企画調査終了報告書のとりまとめ					

５．成果の発信等

(1) 口頭発表

①招待、口頭講演　（国内　2件、海外　0件）

- 松本 勉（横浜国立大学）、富井尚志（横浜国立大学）、物部博文（横浜国立大学）、中川裕志（東京大学）、滝沢修（情報通信研究機構）、井上大介（情報通信研究機構）、赤井健一郎（三菱総合研究所）、佐藤明男（三菱総合研究所）、村瀬一郎（三菱総合研究所）、“ITを用いた子どもの安全確保の構想”、2008年暗号と情報セキュリティシンポジウム、4E1-3、フェニックス・シーガイア・リゾート　ワールドコンベンションセンターサミット、2008年1月22日～25日。
- 松本 勉、“サイバー空間で子供を守るために”、NICT情報通信セキュリティシンポジウム「ネットワーク時代のプライバシとセキュリティ」、SYDホール、2008年2月28日。

②ポスター発表　　（国内　1件、海外　0件）

- パネル展示「ITを用いた子どもの安全確保の研究開発」、2007年度日本大学文理学部特別展「安全を科学する－最新の防犯技術と科学捜査－」2007年12月08日～24日。

(2) その他

特になし。

以上。